D1

then mailed to the customer. As such, from the time the order is placed, considerable time passes before the updated topographical data is actually received by the customer so it can be uploaded into the customer's integrated GPS unit. The delay is even more acute for international customers for which the mailing time is considerably greater.

Replace the first paragraph, Page 9 starting line 1, with the following:

D2

The software layout for the system is illustrated in FIG. 6 and includes a user database 39, a master "nav" database 42 and an upload program 44, identified as NETLOAD.EXE. The user information for example, regarding account and password information, etc. is maintained in the user database 39, accessible by the server 36. The topographical information is stored in the master "nav" database file 42, also accessible by the server 36. Once the user provides the unique software key as well as the desired payment method, a copy of the topographical and/or navigation data from a master "nav" file 42 is encrypted as a function of the unique software key, provided by the user and stored in a "keyed DB file" 44. The keyed DB file 44 is then compressed into a zip file 46 and transferred to the user by way of the Internet along with the decryption or upload file 44, identified as NETLOAD.EXE. The decryption file 44 enables the zip file containing the encrypted database to be uploaded into a product 40 as long as the software key of the product matches the software key to which the database was encrypted. If the software key matches the unique key within the product, the database is decrypted and uploaded into the product.

Replace the last paragraph, Page 11 starting line 29, with the following:

D3

FIG. 14 is a flowchart for the decryption program 44 (NETLOAD.EXE) for uploading the encrypted database software to the GPS unit 40. As mentioned above, the encrypted database file 82 is provided with the encrypted data as well as a footer tag which includes the original software key, checksums, the file size, the database type as well as the effective dates for the database. In step 86, the footer tag is read including the software key from the encrypted output file 82. As discussed in more detail below, the software key from the footer tag is used to decrypt the first byte of the database in step 88. After the first byte is decrypted, the key is updated for the next byte in step 90. After the new key is updated, a checksum is calculated to determine if there are any errors in the data in step 92. The process of steps 88-92 is repeated for each byte in the encrypted database file 82, as indicated by step 94. After all of the bytes in the output file 82 have been decrypted, the system checks in step 96 to determine whether the checksum for the decrypted file matches the original checksum included in the footer tag in the output file 82 in step 96. If

D3

there are any discrepancies in the checksum, an error message is displayed in step 98. If the checksums match, the system communicates with the GPS unit 40 to send an identification packet containing the GPS unit type as well as the software key. Once the software key and GPS unit type are received from the GPS unit 40, the system determines in step 100 whether the GPS unit type matches the database file requested. If not, an error message is displayed in step 102. Otherwise, the system proceeds to step 104 and ascertains whether the software key received from the GPS unit 40 matches the software key used to encrypt the database file and contained in the footer tag mentioned above. If not, an error message is displayed in step 106. Otherwise, the system proceeds to step 108 where the software key received from the GPS unit is used to decrypt the first byte in the output file 82. After the first byte is decrypted or unkeyed, the key is updated in step 110 for the next byte. The steps 108 and 110 are repeated until a sufficient number of bytes have been unkeyed for a full packed as indicated in step 112. Each time a packet is full, a packet of decrypted data is sent to the GPS unit 40 in step 114. As indicated in step 116, the process is repeated until all of the bytes in the encrypted database file have been processed.

IN THE DRAWINGS

Please find attached on a separate sheet revised FIG. 5, with changes to reference numbers shown in red.

IN THE CLAIMS

Cancel Claims 3-24 and add new Claims 25-29.

D4

25. (New Claim) A method for providing to each global positioning (GPS) unit in a plurality of aircrafts software code containing updated aeronautical navigation data, said method comprising the steps of:

assigning to each GPS unit a unique software key;

forwarding a request from one of said GPS units for the updated aeronautical navigation data to a software supplier, said request including the one GPS unit unique software key and payment authorization information;

encrypting the software code for the updated aeronautical navigation data by the supplier in response to said request, said encrypted software code including a decryption program;

transmitting to the one GPS unit said encrypted software code including said decryption program which only allows software to be unloaded into a GPS unit having the unique software key;